

PCPD



H K

個人資料私隱專員公署

Office of the Privacy Commissioner for Personal Data

Data Breach Incidents and Precautionary Measures

HKIoD Directors' Symposium 2024

24 September 2024

Ada CHUNG Lai-ling

Privacy Commissioner for Personal Data

PCPD



H K



[PCPD.org.hk](https://www.pcpd.org.hk)

香港個人資料私隱專員公署
Office of the Privacy Commissioner
for Personal Data, Hong Kong

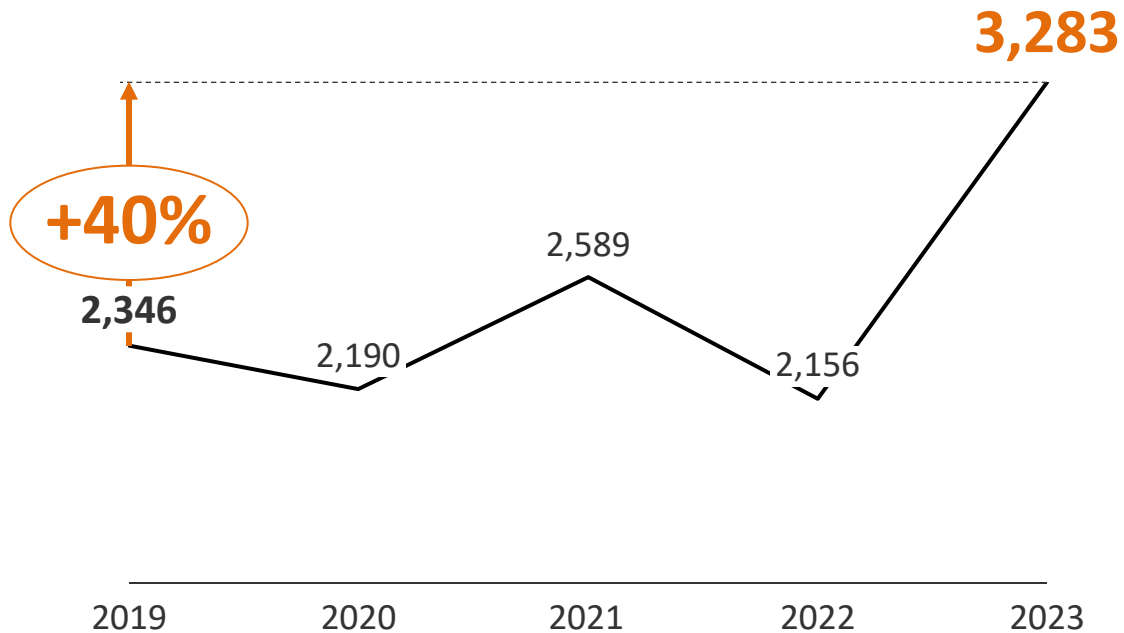
Global Situation

Cyberattacks are rising


 Data breach incidents in the cyber world have risen

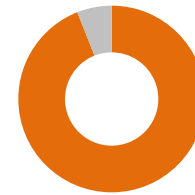
Cyber personal data breach incidents

UK, 2019 – 2023



Source: [ICO](#)

 The prevalence of cyberattacks leave IT professionals sleepless



94%

of **organisations** experienced **cyberattacks** in a global survey



57%

of **IT professionals** **lost sleep** worrying about their organisations being hit by a cyberattack



Source: [Sophos](#)

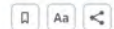
Global Situation

Two incidents indicate the grave consequences of cyberattacks

Casino giant MGM expects \$100 million hit from hack that led to data breach

By Zeba Siddiqui

October 6, 2023 10:35 AM GMT+8 · Updated a year ago



The MGM case (2023)

- Hackers used **vishing (voice phishing)** and **other techniques** to get access to MGM's systems. They then used ransomware to encrypt MGM's data
- Data of customers that used MGM services before 2019, such as **contact information, date of birth and driver's licence numbers**, were leaked
- Took 10 days for MGM to announce that its hotels and casinos resumed operating normally
- **Costs** from the incident **exceeded US\$110 million**

Source: [Reuters \(2023\)](#); [Security Week \(2023\)](#); [Vox \(2023\)](#); [Z Cybersecurity](#)

Medibank says hacker accessed data of 9.7 million customers, refuses to pay ransom

Reuters

September 15, 2022 10:35 AM GMT+8 · Updated a year ago



The Medibank case (2022)

- Hackers used the **credential stolen** from an account to gain preferential access to the internal system of the insurer, resulting in the **health data of over 9 million customers released on the dark web**
- Australian Information Commissioner filed civil penalty proceedings against Medibank in June 2024 for **failing to take reasonable steps to protect Australians' personal data from misuse and unauthorised access or disclosure**

Source: [Reuters \(2022\)](#), [OAIC \(2024\)](#)

PCPD




HK

PCPD.org.hk

香港個人資料私隱專員公署
Office of the Privacy Commissioner
for Personal Data, Hong Kong

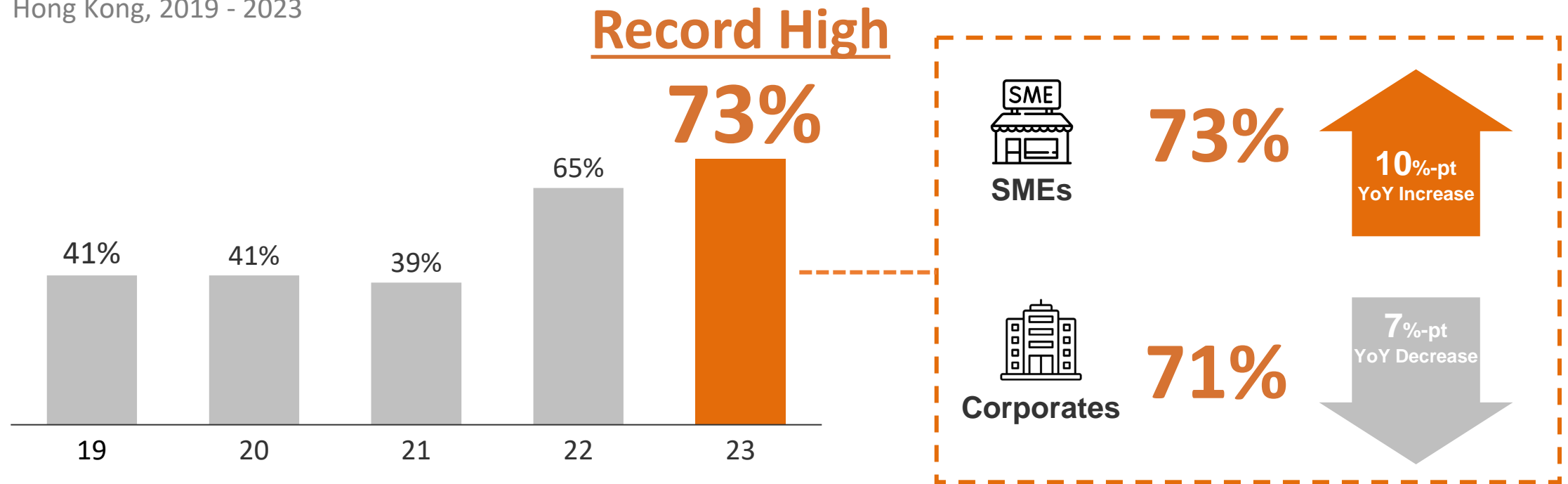
Local Cyber Attacks

Cyberattacks are also increasing in Hong Kong

 PCPD's survey with HKPC shows nearly $\frac{3}{4}$ of enterprises faced cyberattacks in 2023, the highest in five years

% of enterprises that encountered cyberattacks in the past 12 months

Hong Kong, 2019 - 2023



Source: Hong Kong Enterprise Cyber Security Readiness Index

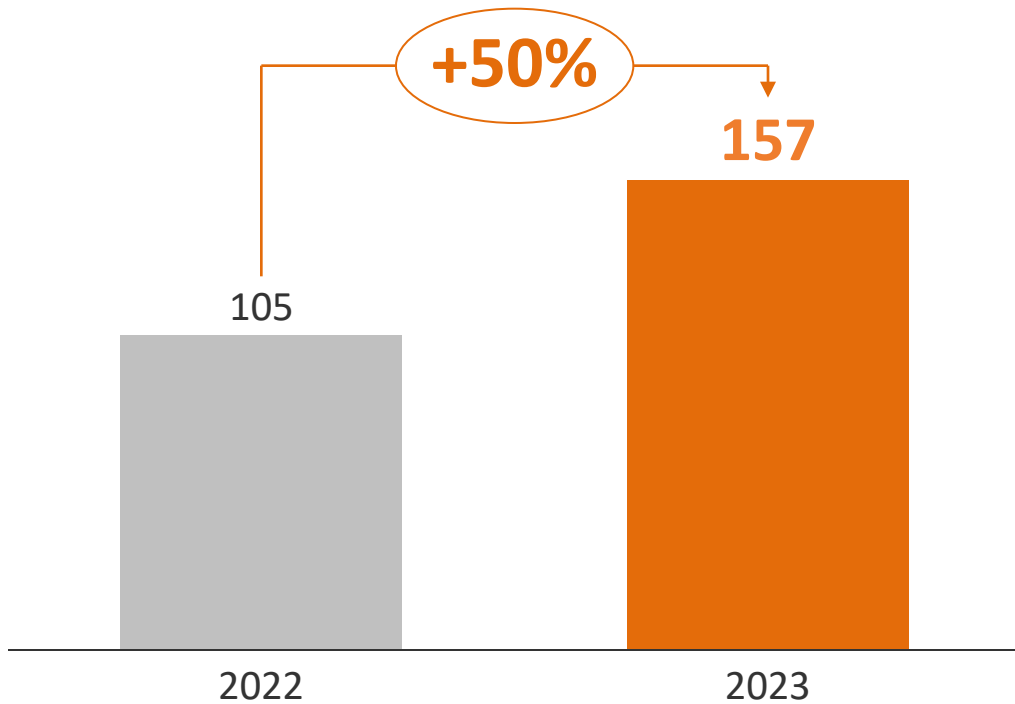
4

Local Data Breaches

Data breach notifications rose in 2023; hacking was a major contributor

 Compared to 2022, DBNs in 2023 rose substantially by 50%

Data breach notifications to PCPD

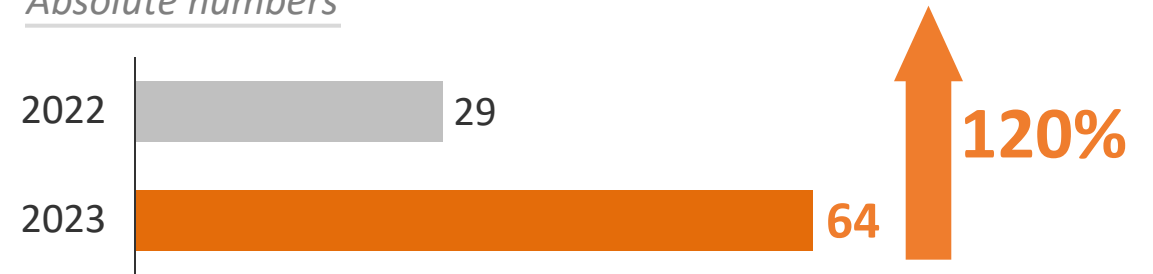


Source: PCPD

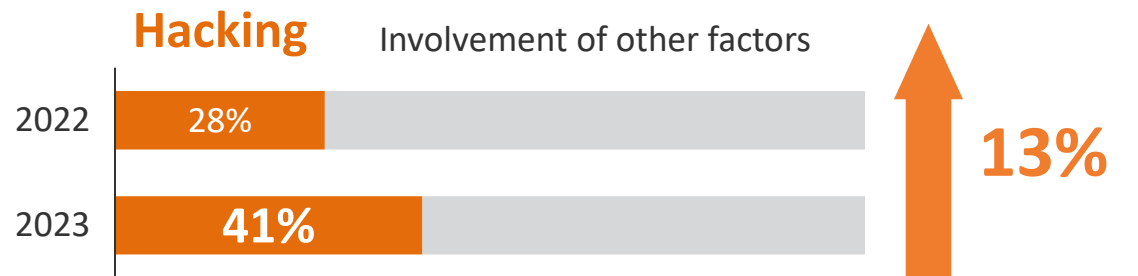
 DBNs involving hacking rose both absolutely and relatively

Data breach notifications involving hacking

Absolute numbers



As a percentage of total



Legal Liability

Security of personal data

DPP4(1)



A data user shall take **all reasonably practicable steps** to ensure that the personal data it holds is protected against unauthorised or accidental access, processing, erasure, loss or use.

DPP4(2)



If a data user engages a data processor, whether within or outside Hong Kong, to process personal data on the data user's behalf, the **data user must adopt contractual or other means**, to prevent unauthorised or accidental access, processing, erasure, loss or use of the data transferred to the data processor for processing.

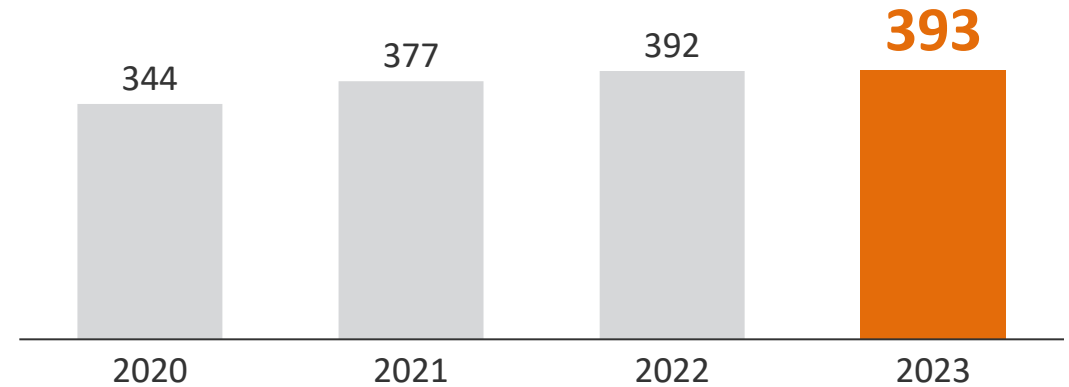
Inspections and Compliance Checks

PCPD takes proactive actions

Inspections by PCPD in the past 3 years

| Report Date | Companies Inspected |
|-------------|---|
| Oct 23 | ZA Bank Limited |
| Sep 23 | The Registration and Electoral Office |
| Dec 22 | TransUnion Limited |
| Aug 21 | (1) CLP Power Hong Kong Limited and (2) The Hongkong Electric Company, Limited |

Compliance checks initiated by PCPD



Selected compliance checks launched in 2023

- All **credit reference agencies**
- **Users of AI systems**

Investigation into an Online Shopping Platform

Unauthorised scraping of personal data of the platform's users

Background



Data Breach Notification

The investigation arose from **a notification lodged by the company operating the online shopping platform** (the Company)

2.6 million

Personal data of 2.6 million users **posted for sale**

324,232

No. of **Hong Kong users** affected

Details



Security Vulnerability relating to a System Migration

Cause of the data breach incident found by our investigation



The Company's Obligation as a Data User

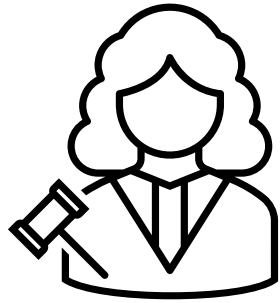
The Company has a positive duty to safeguard the security of the personal data under its control

Investigation into an Online Shopping Platform

Decision



DPP4(1) contravention



The Company had **not taken all practicable steps** in relation to the system migration to ensure that the **personal data held by the Company were protected from unauthorised or accidental access, processing, erasure, loss or use**, thereby contravening DPP 4(1) concerning the **security of personal data**



The Privacy Commissioner served an **Enforcement Notice** on the Company, directing it to **remedy and prevent recurrence of the contravention**

PCPD's Resources for Enhancing Data Security

PCPD is helping data users enhance data security and prevent data breaches

Data Security Thematic Webpage

One-stop access to resources on data security



Data Security Scanner

Self-assessment toolkit for enterprises to assess adequacy of data security measures of ICT systems



Data Security Hotline

Provide SMEs with a channel to make enquiries about compliance with the PDPO



Guidance Materials

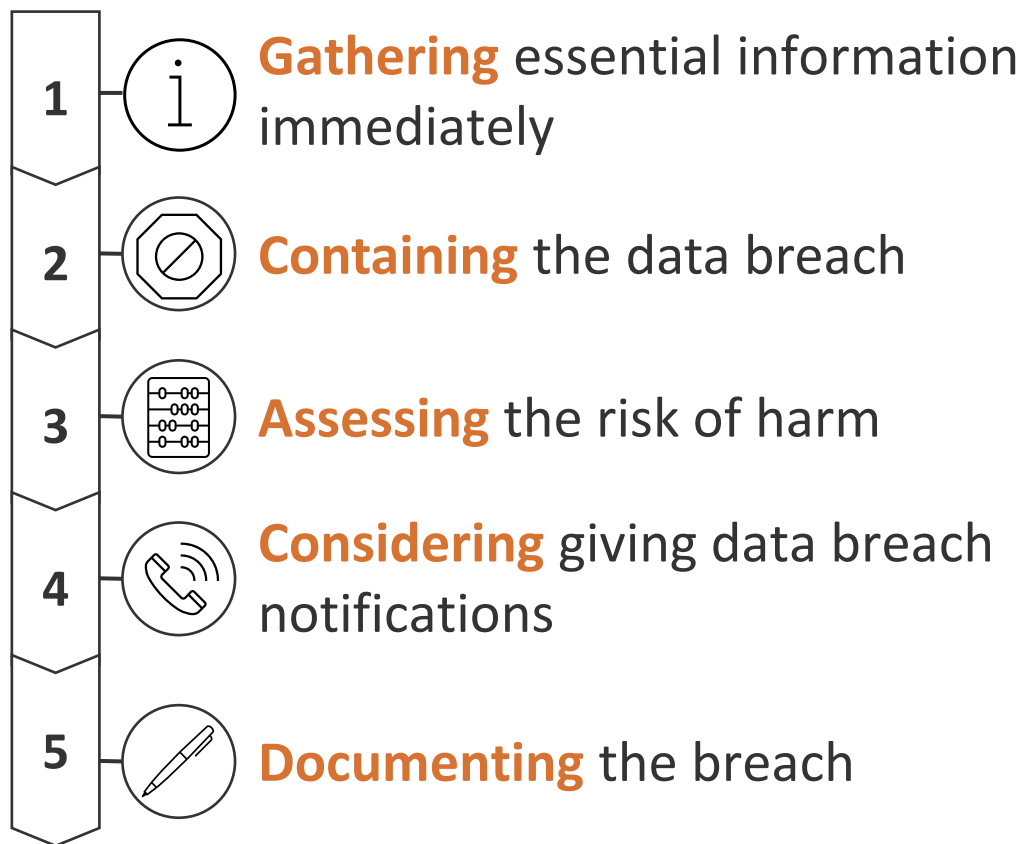
- **Data Breach Response Plan**
- **Guidance Note on Data Security Measures for ICT**
- **Privacy Management Programme (PMP)**

Handling Data Breaches

Handling a data breach requires 5 steps, with a preparatory plan in place



Steps to take when handling data breaches



Data Breach Response Plan

Putting a plan in place can help minimise impact of a data breach

What



A document setting out **how** an organisation should **respond in a data breach**



The plan should outline:











- a **set of procedures** to be followed in a data breach
- **strategy for identifying, containing, assessing and managing** the impact brought about by the incident from start to finish

Why



Help ensure a **quick response** to and **effective management** of a data breach

Elements

-  Description of what makes a data breach
-  Internal incident notification procedure
-  Contact details of response team members
-  Risk assessment workflow
-  Containment strategy
-  Communication plan
-  Investigation procedure
-  Record keeping policy
-  Post-incident review mechanism
-  Training or drill plan

Guidance Note on Data Security Measures for ICT

We recommend best practices in strengthening data security

Background



We have witnessed an **increasing number of data breaches** over the years



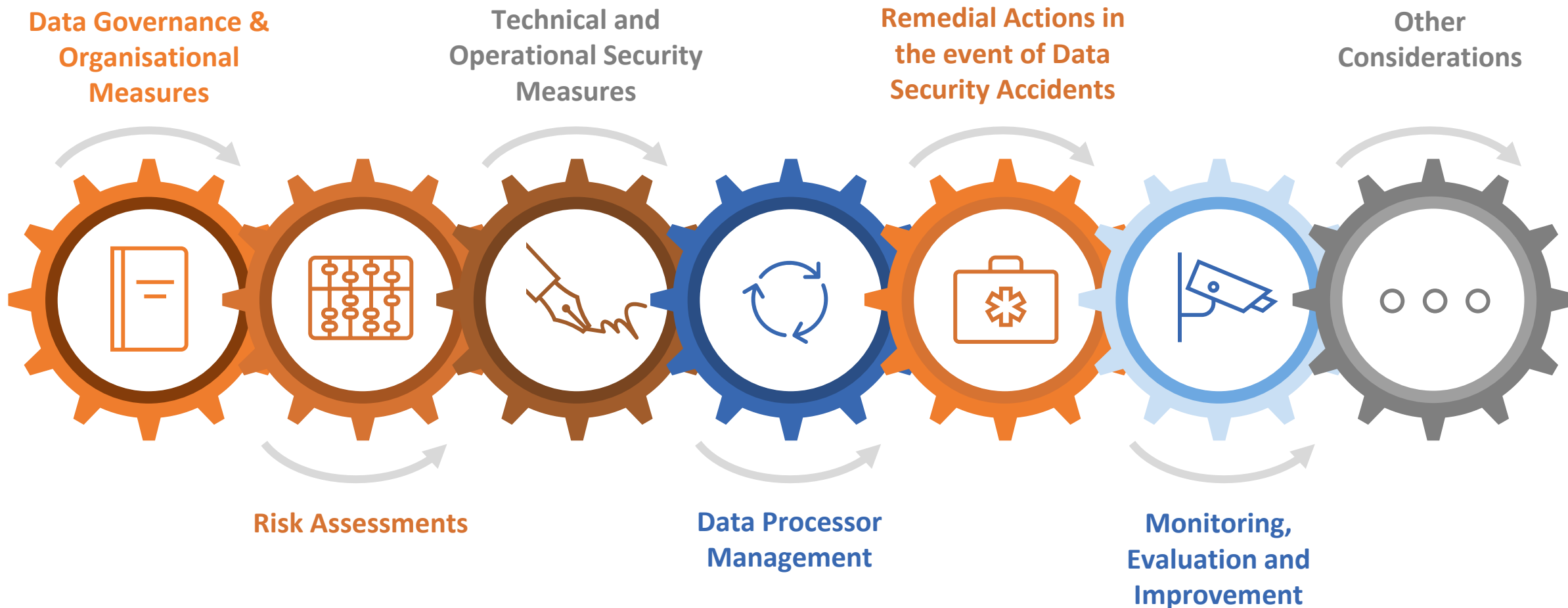
Data users should step up their data security measures to **prevent malicious attacks** on their information systems



Robust data security system is a core element of **good data governance**

7 Recommended Measures

Taking the below measures enhances data security of organisations



Privacy Management Programme (PMP)

Definition and benefits of adoption



What's PMP

A **management framework**

- For the **responsible collection, holding, processing & use of personal data** by the organisation
- To **ensure compliance with Personal Data (Privacy) Ordinance (PDPO)**

Why PMP



Minimise risk of data security incidents



Handle data breaches effectively to minimise damage



Ensure compliance with PDPO



Build trust with employees and customers, and enhance corporate reputation and competitiveness

“**Guide for Independent Non-Executive Directors**” published by HKIoD recommends use of **PMP** as part of **ESG management**!



15

PCPD



PCPD.org.hk

香港個人資料私隱專員公署
Office of the Privacy Commissioner
for Personal Data, Hong Kong



Thank you!



www.pcpd.org.hk

communications@pcpd.org.hk



Please follow us!

